

Inicio de sesión de Secure Malware Analytics con Cisco Security Cloud Sign-On (Cisco SCSO): cómo vincular cuentas

Contenido

[Introducción](#)

[Creación de un nuevo usuario SMA](#)

[Vincular usuario existente](#)

[Varias cuentas Secure Malware Analytics vinculadas a una única cuenta SCSO](#)

[Inicio de sesión solo de SCSO para la integración](#)

[Support](#)

Introducción

Este documento describe cómo Secure Malware Analytics (SMA) realizará la transición a Security Cloud Sign On (SCSO) como el método de autenticación exclusivo para todos los usuarios. Este cambio pretende proporcionar una experiencia de inicio de sesión coherente y centralizada en todos los productos de seguridad de Cisco.

Este documento describe los cambios introducidos por esta transición y explica cómo los usuarios pueden vincular su cuenta SCSO a Secure Malware Analytics. Esta función estará disponible a partir del 19 de febrero de 2026.

Después de esta fecha, ya no se admitirá la autenticación mediante nombres de usuario y contraseñas SMA nativos.

Inicio de sesión en la nube de seguridad (SCSO)

Cisco Security Cloud Sign-On es un servicio de gestión de identidades centralizado diseñado para proporcionar una experiencia de inicio de sesión unificada y muy segura en varias aplicaciones de seguridad de Cisco. Se puede utilizar una única cuenta SCSO para acceder a varios servicios de seguridad de Cisco.

Todos los usuarios deben tener una cuenta registrada de Cisco SCSO para acceder a Secure Malware Analytics.

Para registrarse en Cisco SCSO, vaya a: <https://sign-on.security.cisco.com/signin/register>

Creación de un nuevo usuario SMA

El proceso para crear un nuevo usuario en Secure Malware Analytics no se modifica, incluido el hecho de que se envía automáticamente un correo electrónico de invitación de vinculación de

cuenta después de la creación del usuario.

Crear nuevo usuario:

1. Inicie sesión en Secure Malware Analytics como administrador de la organización.
2. Vaya a Administration > Users > New User.
3. Introduzca la información necesaria:
 - Inicio de sesión
 - Función
 - User Name
 - Correo electrónico
4. Haga clic en Enviar.

New User

Active User Quota: 4/10 ⓘ

Organization

SMA, [REDACTED] Test_Org

Login *

test_user04

Role *

User

User Name *

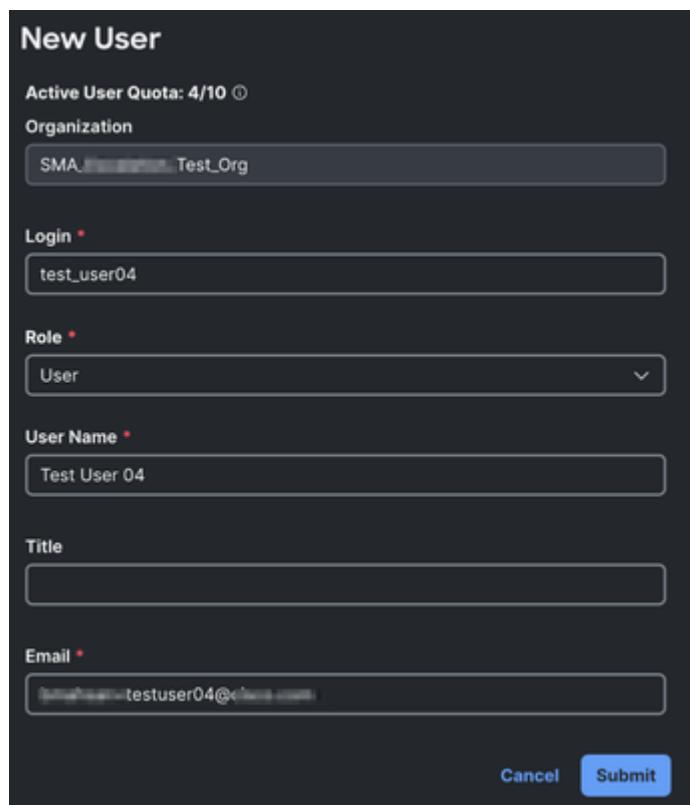
Test User 04

Title

Email *

testuser04@[REDACTED]

[Cancel](#) [Submit](#)



Vinculación de una nueva cuenta de usuario a una cuenta SCSO:

Se crea la cuenta de usuario y se envía un correo electrónico de invitación titulado "Secure Malware Analytics (SMA) SCSO Link Request" desde noreply@cisco.com a la dirección de correo electrónico del usuario.

Secure Malware Analytics (SMA) SCSO Link Request

N

○ noreply@cisco.com <noreply@cisco.com>

To: [REDACTED] testuser04@[REDACTED]

Today at 10:32 AM

Cisco Secure Malware Analytics

Secure Malware Analytics (SMA) SCSO Link Request

Someone has requested to link a Security Cloud Sign On account to your Malware Analytics account with the login: test_user04

If this was you, then please open the following URL in your browser:

[https://\[REDACTED\].threatgrid.com/sso/users/link_confirm?token=\[REDACTED\]](https://[REDACTED].threatgrid.com/sso/users/link_confirm?token=[REDACTED])

This will link the accounts.

THIS TOKEN WILL EXPIRE IN 36 HOURS

If your token has expired, please request a new token by opening the following URL in your browser: [Link Request Link](#)

If you have any problems accessing SMA, then please contact your SMA administrator immediately.

Thank you,
Secure Malware Analytics Team
Cisco Secure Malware Analytics

Need to report an issue? [Open a support case](#)

© 2026 Cisco Systems Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems Inc. and/or its affiliates in the U.S. and certain other countries.

Cuando el usuario haga clic en la URL o la abra en su navegador, se le redirigirá a la página de inicio de sesión en la nube de seguridad (SCSO).

Si el usuario ya se ha registrado en la cuenta de SCSO, se autenticará mediante su dirección de correo electrónico registrada y vinculará su cuenta SMA.

Si el usuario no tiene una cuenta SCSO, seleccione Sign up now (Registrarse ahora) para iniciar el proceso de registro.

Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)



Or

[Other login options](#)

[System status](#) [Policy statement](#)

Introduzca la información de cuenta para suscribirse a una cuenta de SCSO. El usuario recibe un correo electrónico para activar la nueva cuenta de SCSO. Siga las instrucciones del correo electrónico para activar la cuenta y habilitar la autenticación multifactor.

Account Sign Up

Provide following information to create organization account.
[Back to login page](#)

Email *

First name *

Last name *

Country *

Password * [Show](#)

Confirm Password * [Show](#)



Security Cloud Sign On

Activate Account

By accept, you agree that your use of this Cisco Offer, and any Cisco Offers managed through this Cisco Offer, is governed by Cisco's General Terms, and any applicable Offer Description(s) and Supplemental Terms. You also acknowledge that you have read the Cisco Privacy statement.

[Sign up](#)

[Cancel](#)

Una vez que el usuario se haya registrado correctamente para obtener una cuenta de SCSO, vuelva al correo electrónico de solicitud de enlace de SCSO de Secure Malware Analytics (SMA) recibido anteriormente y abra la URL en un navegador.

Después de la autenticación correcta, se presenta al usuario la opción de vincular la cuenta SMA con la cuenta SCSO iniciada.

Confirm Link Accounts

You are logged into Security Cloud Sign On as:

~~XXXXXXXXXX~~+testuser04@~~XXXXXXXXXX~~.com

This Security Cloud Sign On account will be linked to the Malware Analytics account: test_user04

Confirm

Confirme la acción. Se muestra un mensaje de confirmación que indica "Se han vinculado sus cuentas". Seleccione Continuar con el inicio de sesión en la nube de seguridad para iniciar sesión en la cuenta de Secure Malware Analytics (SMA) y acepte el Acuerdo de licencia del usuario final (EULA) para completar la configuración de la cuenta.

i Your accounts have been linked!

i Security Cloud Sign On is enabled

You will need a Security Cloud Sign On account to log in.

[Learn how to set up an account.](#) 

Log in

Log in to your Secure Malware Analytics account.

Continue with Security Cloud Sign On

Vincular usuario existente

Si una cuenta existente de Secure Malware Analytics (SMA) no se ha vinculado a Security Cloud Sign On (SCSO) antes de que la función de inicio de sesión solo de SCSO entre en vigor el 19 de

febrero de 2026, realice el siguiente procedimiento para vincular las cuentas.

Requisito previo

Se necesita una cuenta registrada de Security Cloud Sign On (SCSO).

Si no se ha creado una cuenta de SCSO, regístrate en: <https://sign-on.security.cisco.com/signin/register>

Procedimiento

Navegue hasta el portal de Secure Malware Analytics apropiado:

- EE. UU.: <https://panacea.threatgrid.com>
- UE: <https://panacea.threatgrid.eu>
- Australia: <https://panacea.threatgrid.com.au>
- Canadá: <https://panacea.threatgrid.ca>

En la pantalla de inicio de sesión, seleccione Continue with Security Cloud Sign On para iniciar sesión mediante SCSO.

 Security Cloud Sign On is enabled

You will need a Security Cloud Sign On account to log in.

[Learn how to set up an account.](#) 

Log in

Log in to your Secure Malware Analytics account.

[Continue with Security Cloud Sign On](#)

Inicie sesión en Security Cloud Sign On (SCSO) con la cuenta creada anteriormente.

Security Cloud Sign On

Email

[Continue](#)

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

[System status](#) [Policy statement](#)

Después de la autenticación correcta, aparece un mensaje que indica "No hay cuentas de análisis de malware vinculadas a esta cuenta de SCSO". junto con la opción de vincular una cuenta.

Seleccione Vincular una cuenta para empezar a vincular la cuenta de Secure Malware Analytics (SMA) existente a la cuenta de SCSO.

Select account

You are logged into Security Cloud Sign On as:

existinguser01@cisco.com

[Log out of Security Cloud Sign On](#)

 There are no Malware Analytics accounts linked to this SCSO account.

Missing an account? Make sure you are logged into the correct Security Cloud Sign On account. [Link an account.](#)



En la página siguiente, se muestra una opción para vincular cuentas. Introduzca el nombre de usuario existente y seleccione el enlace Solicitar.

Link accounts

Enter the Malware Analytics username to link to this Security Cloud Sign On account.

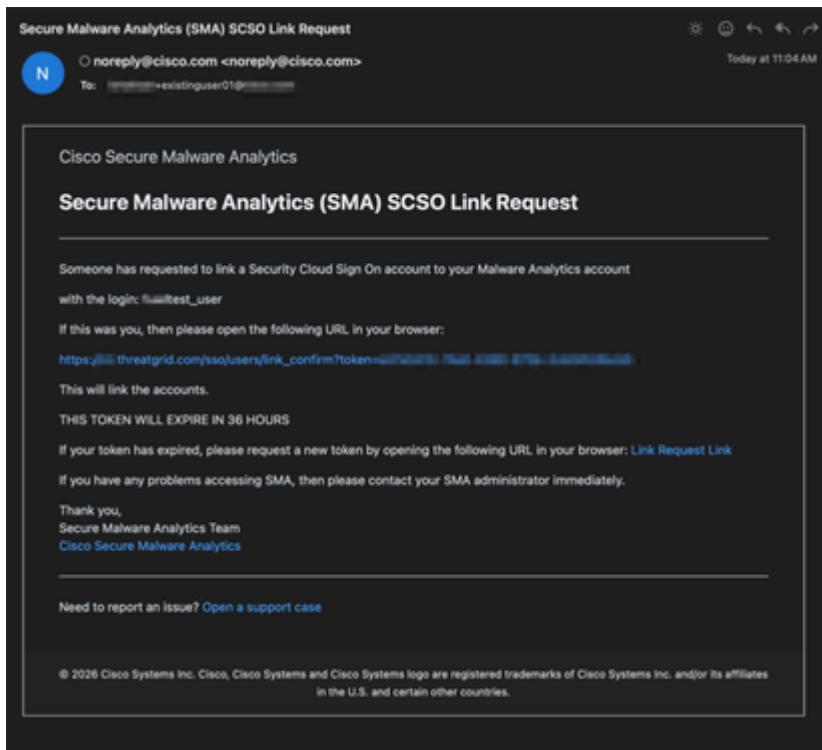
Username

Request link



Se envía un correo electrónico de invitación a la dirección de correo electrónico configurada para la cuenta existente.

En la mayoría de los casos, esta dirección de correo electrónico coincide con la dirección de correo electrónico de la cuenta SCSO. Si debe actualizar la dirección de correo electrónico, póngase en contacto con el administrador de la organización o con el equipo de asistencia de Cisco.



Abra la URL proporcionada en el correo electrónico de invitación en un navegador. Después de la autenticación correcta, se le pide al usuario que confirme la vinculación de la cuenta.

Verifique los detalles de la cuenta y seleccione Confirm.

Confirm Link Accounts

You are logged into Security Cloud Sign On as: [REDACTED]+existinguser01@[REDACTED].com

This Security Cloud Sign On account will be linked to the Malware Analytics account:
[REDACTED]test_user

[Confirm](#)

Se muestra un mensaje de confirmación que indica que las cuentas se han vinculado. Seleccione Continuar con el inicio de sesión en la nube de seguridad para iniciar sesión en la cuenta existente de Secure Malware Analytics mediante SCSO.

i Your accounts have been linked!

i Security Cloud Sign On is enabled

You will need a Security Cloud Sign On account to log in.

[Learn how to set up an account.](#) 

Log in

Log in to your Secure Malware Analytics account.

[Continue with Security Cloud Sign On](#)

En la página siguiente, seleccione la cuenta de usuario en la que desea iniciar sesión.

Select account

You are logged into Security Cloud Sign On as:

[REDACTED]+existinguser01@[REDACTED].com

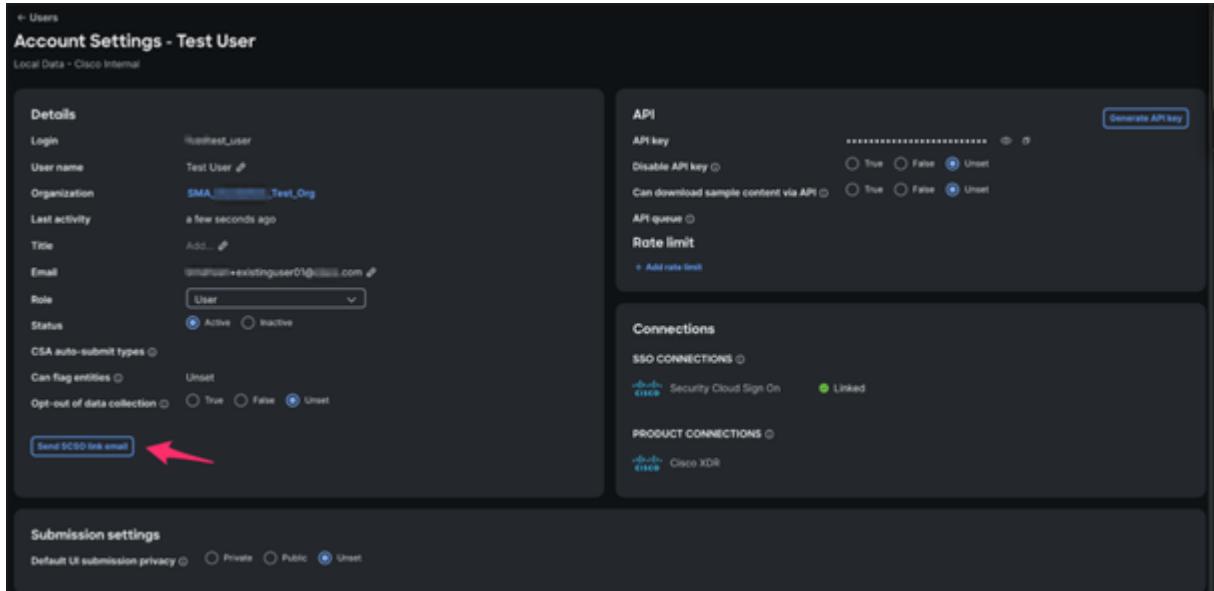
[Log out of Security Cloud Sign On](#)

User

[REDACTED]test_user

Missing an account? Make sure you are logged into the correct Security Cloud Sign On account. [Link an account.](#)

Nota: Los administradores de la organización también pueden enviar el correo electrónico de invitación de enlace de la cuenta de SCSO desde la página Administración de usuarios.



The screenshot shows the 'Account Settings - Test User' page. The 'Details' section includes fields for Login (test_user), User name (Test User), Organization (SMA_XXXX_Text_Org), Last activity (a few seconds ago), Title (Add...), Email (testuser+existinguser01@XXXX.com), Role (User), Status (Active), CSA auto-submit types (Unset), Can flag entities (Unset), and Opt-out of data collection (Unset). The 'API' section shows an API key (disabled), API quota (Unset), and Rate limit (Unset). The 'Connections' section shows SSO CONNECTIONS (Security Cloud Sign On: Linked) and PRODUCT CONNECTIONS (Cisco XDR). At the bottom, there is a 'Send SCSO link email' button, which is highlighted with a red arrow.

Varias cuentas Secure Malware Analytics vinculadas a una única cuenta SCSO

Los usuarios pueden vincular varias cuentas de Secure Malware Analytics (SMA) a la misma cuenta de inicio de sesión en la nube de seguridad (SCSO) mediante el método Create New SMA User o Link an Existing User.

Después de una autenticación de SCSO correcta, se presenta al usuario una opción para seleccionar la cuenta de Secure Malware Analytics a la que acceder.

Select account

You are logged into Security Cloud Sign On as:

1@XXXX.com

[Log out of Security Cloud Sign On](#)

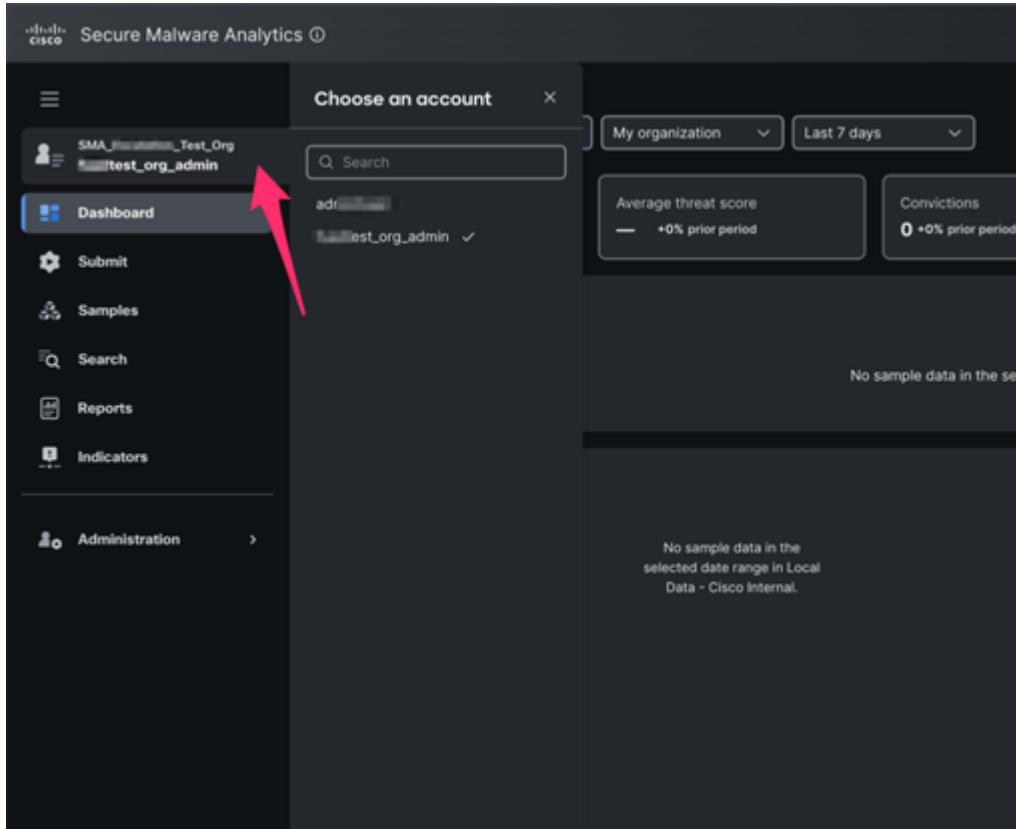
User

[test_org_admin](#)



Missing an account? Make sure you are logged into the correct Security Cloud Sign On account. [Link an account](#).

Los usuarios también pueden cambiar entre cuentas después de iniciar sesión mediante el menú de navegación de la izquierda.



Inicio de sesión solo de SCSO para la integración

Las integraciones como Umbrella SIG, Secure Access, Meraki y Email Threat Defence (ETD) aprovisionan automáticamente una cuenta de administrador de organización o administrador de dispositivo cuando se registran en Secure Malware Analytics.

Se envía un correo electrónico de invitación a la dirección de correo electrónico proporcionada por el dispositivo o servicio integrador para completar el enlace de la cuenta mediante el inicio de sesión en la nube de seguridad (SCSO).

Support

Para obtener asistencia o información adicional, póngase en contacto con el [centro de asistencia técnica Cisco Technical Assistance Center \(TAC\)](#).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).